(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENTAMT

(12) **Offenlegungsschrift**

(10) **DE 42 25 345 A 1**

(51) Int. Cl.[5]: G 06 F 12/14

(21) Aktenzeichen: P 42 25 345.4
(22) Anmeldetag: 31. 7. 92
(43) Offenlegungstag: 3. 2. 94

DE 42 25 345 A 1

(71) Anmelder:
Drozd, Igor, Dipl.-Ing., 65618 Selters, DE

(74) Vertreter:
Blumbach, P., Dipl.-Ing., 65193 Wiesbaden; Weser, W., Dipl.-Phys. Dr.rer.nat.; Kramer, R., Dipl.-Ing., 81245 München; Zwirner, G., Dipl.-Ing. Dipl.-Wirtsch.-Ing., 65193 Wiesbaden; Hoffmann, E., Dipl.-Ing., Pat.-Anwälte, 82166 Gräfelfing

(72) Erfinder:
gleich Anmelder

(54) Verfahren zum Schutz von MS-DOS-Rechnern gegen Sabotageprogramme oder »Viren«

(57) Es wird ein Verfahren beschrieben, mit dem sich MS-DOS-Rechner gegen Sabotageprogramme oder sogenannte "Viren" schützen lassen. Anders als bei bekannten Verfahren können nicht nur bereits bekannte Viren in Form bestimmter Zeichenketten in den Dateien und im Speicher festgestellt und dann beseitigt werden, sondern es lassen sich auch Sabotageversuche mit unbekannten Virussignaturen erkennen, so daß sie bei der Aktivierung keinen Schaden anrichten können. Dazu wird bei Aufruf von sektororientierten Funktionen zunächst geprüft, ob der Aufruf vom Kern des Betriebssystems ausgeht. Ist das der Fall, so wird der Aufruf zugelassen. Im anderen Fall wird geprüft, ob der Aufruf von einem zugelassenen Dienstprogramm kommt. Ist dies der Fall, wird wiederum der Aufruf zugelassen. Im anderen Fall wird die Ausführung gesperrt und dem Rechnerbenutzer eine Warnung ausgegeben, beispielsweise ein optisch auffallendes Warnfenster auf dem Bildschirm des Rechners.

DE 42 25 345 A 1

Beschreibung

Im Hinblick auf die massive Verbreitung von Virus- und Sabotageprogrammen aller Art gewinnt die Tatsache an Bedeutung, daß die Systembereiche von Datenträgern, insbesondere Festplatten und Disketten, beim Betriebssystem MS-DOS gegen eine mutwillige Zerstörung nicht geschützt sind. Die bekannten Anti-Virus-Verfahren beschränken sich auf die Erkennung sogenannter Virus-Signaturen in Form bestimmter Zeichenketten in den Dateien und im Speicher. Der große Nachteil solcher Verfahren besteht darin, daß sie sich naturgemäß auf die schon bekannten Viren beschränken müssen. Insbesondere können sie das Anrichten von Schäden nicht verhindern, falls ein unbekannter Virus aktiv wird. Das Erkennen der Virus-Signaturen ist auch noch dadurch schwieriger geworden, daß inzwischen polymorphe Viren auftreten, also solche Viren, die ihre Signatur selbst ändern können.

Zur Verdeutlichung der Gefahren, die das ungeschützte MS-DOS-System bedrohen, sei erläutert, daß bereits kurze Programmfragmente mit einer Gesamtlänge von beispielsweise 8 Bytes und einer Ausführungszeit von nur wenigen Millisekunden jeden Zugriff zur Festplatte eines Rechners und sogar das Hochziehen (Booten) des Betriebssystems verhindern können. Eine Restaurierung der auf diese Weise zerstörten Festplatte ist, wenn überhaupt, nur von Experten in mühevoller und zeitraubender Handarbeit möglich.

Der Erfindung liegt demgemäß die Aufgabe zugrunde, ein Verfahren anzugeben, das Betriebssystem MS-DOS so zu schützen, daß Sabotageversuche auch mit unbekannten Virussignaturen zwar nicht verhindert werden, aber bei der Aktivierung keinen Schaden anrichten, insbesondere keine vitalen Systembereiche der Datenträger überschreiben und dadurch zerstören können. Die Lösung der Aufgabe ist im Patentanspruch 1 angegeben.

Der Erfindung liegt das Prinzip zugrunde, vor der Ausführung von potentiell gefährlichen Zugriffen auf Systembereiche von Datenträgern, die bisher vom Betriebssystem MS-DOS ohne jede Sicherheitsprüfung durchgeführt wurden, den Anwender zu warnen, falls keine offensichtlich systembedingte Notwendigkeit für einen solchen Zugriff besteht. Zur näheren Erläuterung des erfindungsgemäßen Verfahrens soll zunächst das MS-DOS-Betriebssystem im hier interessierenden Zusammenhang kurz erläutert werden.

MS-DOS bietet grundsätzlich zwei Gruppen von Programmierfunktionen, die der Manipulation von Datenträgern, also Festplatten oder Disketten, dienen können, nämlich dateiorientierte und sektororientierte Funktionen. Da ein Anwendungsprogramm im Normalfall ausschließlich dateiorientierte Operationen ausführen darf und ein Datenträger nur aus einzelnen Sektoren, Zylindern und Köpfen besteht, sorgt der MS-DOS-Kern bei jeder dateiorientierten Operation für die transparente Umsetzung des logischen Begriffs "Datei" in die physikalischen Werte "Sektor", "Zylinder" usw. Darüber hinaus muß der Kern bei jeder dateiorientierten Operation ebenfalls transparent auch den Systembereich verwalten.

Ein Datenträger besteht, vereinfacht dargestellt, aus dem Systembereich und dem Datenbereich. Der Systembereich einer typischen Festplatte enthält, wiederum schematisch, einen Partition-Sektor, einen Boot-Sektor und zwei Kopien einer Dateizuordnungstabelle FAT (von File Allocation Table). Zum Systembereich lassen sich auch noch das Wurzel-(Root)-Verzeichnis sowie die drei zum Booten notwendigen Dateien IO.SYS, MSDOS.SYS und COMMAND.COM hinzurechnen. Unter dem Aspekt der Sicherheit ist folgendes zum Systembereich wichtig: Der Systembereich ist unabdingbar für die richtige Funktion des Systems, er ist relativ klein im Vergleich zum Datenbereich, und er sollte nur vom MS-DOS-Kern verwaltet und modifiziert werden. Die letzte Bedingung wird von MS-DOS selbst verletzt, da einige Systemfunktionen, z. B. das Formatieren von Datenträgern, das-Anlegen einer Partition usw. , vom Kern in externe Dienstprogramme verlegt wurden. Diese Dienstprogramme sind zwar formal Bestandteil von MS-DOS, nicht aber vom Kern, der also deren Aktivitäten nicht überwachen und kontrollieren kann. Der MS-DOS-Kern bietet deshalb einige sektororientierte Funktionen, um diesen Dienstprogrammen den Zugriff zum Systembereich zu ermöglichen. Im wesentlichen handelt es sich dabei um die Funktionen "Absolute Disk Read" und "Absolute Disk Write", d. h. die Interrupts 25 und 26 (in hexadezimaler Schreibweise).

Bei alleiniger Verwendung von dateiorientierten Funktionen lassen sich Schäden kaum anrichten. Ein Sabotageprogramm hat auf diese Weise keinen Zugriff zum Systembereich und könnte höchstens Dateien überschreiben oder löschen. Da dem Sabotageprogramm die Namen von Dateien und Verzeichnissen in der Regel unbekannt sind, müßte sich das Sabotageprogramm blind durch die Dateien hindurcharbeiten. Das wäre zeitaufwendig und auffällig. Außerdem könnte der geschädigte Anwender gelöschte Dateien sofort wiederherstellen, z. B. durch das Dienstprogramm "UNDELETE".

Einen echten und nicht wiederherstellbaren Schaden kann ein Sabotageprogramm allein durch die sektororientierten Funktionen anrichten. Daher findet die Prüfung gemäß Merkmal a) im Anspruch 1 für diese Funktionen statt.

Jeder Versuch, eine sektororientierte Funktion aufzurufen, ist sabotageverdächtig, sofern der Aufruf nicht von MS-DOS selbst, also vom Kern oder von bestimmten, zugelassenen Dienstprogrammen stammt, sondern von einem Applikationsprogramm. Daher die Prüfungen gemäß Verfahrensschritt a) und c) im Anspruch 1.

Insgesamt gibt es bei den sektororientierten Funktionen nur sechs mögliche Angriffspunkte für Sabotageprogramme, nämlich

a) durch Aufruf der Funktion "ABSOLUTE DISK WRITE" (Interrupt 26),
b) durch Aufruf von Festplatten- oder Disketten-Gerätetreibern,
c) durch Aufruf der Funktion "EXECUTE DEVICE DRIVER REQUEST" (Interrupt 2f, Funktion 0802),
d) durch Aufruf der Funktion "GENERIC BLOCK DEVICE REQUEST" (Interrupt 21, Funktion 440d),
e) durch Aufruf der Funktion "ROM-BIOS Fixed Disk" (Interrupt 13)
f) durch direkten Sprung zur ursprünglichen ROM-Adresse von der Funktion "ROM-BIOS Fixed Disk", feststellbar durch die Funktion "SET DISK INTERRUPT HANDLER" (Interrupt 2f, Funktion 13).

Diese möglichen Angriffspunkte, die eine vollständige Aufstellung darstellen, sind auch Gegenstand von Weiterbildungen der Erfindung.

Zur Durchführung des Verfahrensschrittes c) wird zu-

nächst der Name des aufrufenden Programms festgestellt, beispielsweise bei zugelassenen Programmen "FORMAT" oder "FDISK". Da aber ein Sabotageprogramm ziemlich leicht auch den Programmnamen in der Programmumgebung modifizieren könnte, um ein erlaubtes Programm vorzutäuschen, wird mit Vorteil bei Aufrufen der Funktion "LOAD AND EXECUTE A PROGRAM", auch EXEC-Funktion genannt, der Name des auszuführenden Programms abgespeichert und mit dem Namen des aufrufenden Programms verglichen. Die beiden Namen müssen übereinstimmen, sonst wird die Warnung ausgegeben.

Bei Aufruf der Funktionen "ABSOLUTE DISK WRITE", "GENERIC BLOCK DEVICE REQUEST" und "ROM-BIOS FIXED-DISK" wird jeweils der zugehörige Interrupt, beispielsweise Interrupt 26 für "ABSOLUTE DISK WRITE" während der Initialisierungsphase umgeleitet, der Name des aufrufenden Programms geprüft und dann zum ursprünglichen Interrupt zurückgekehrt.

Beim Aufruf eines Plattentreibers wird zunächst festgestellt, ob es sich um einen Schreibzugriff auf den Systembereich handelt. Um dann zu prüfen, ob der Zugriff vom Kern kommt, wird festgestellt, ob zur Zeit eine MS-DOS-Funktion ausgeführt wird und ob sich die Transferadresse, also die Adresse, aus der die Daten auf die Platte geschrieben werden sollen, auf einen Kern-Datenpuffer bezieht. Zur Durchführung wird dazu der Plattentreiberaufruf dadurch umgeleitet, daß bei der Initialisierung ein neuer Plattentreiber angelegt wird, der die Prüfungen ausführt und bei positivem Ausgang den bisherigen Plattentreiber zur Ausführung des Zugriffs aufruft.

Die Ausgabe einer Warnung umfaßt zweckmäßig die Ausgabe eines optisch auffallenden Warnfensters auf dem Bildschirm des Rechners. Dabei gibt das Warnfenster jeweils die Ursache für die Warnung und gegebenenfalls weitere Einzelheiten für Diagnosezwecke, beispielsweise den vollen Pfadnamen des Verursachers, die physikalische Adresse des beanstandeten Aufrufs, die Registerinhalte, den System- und den Anwender-Stack, usw. Außerdem kann das Warnfenster ein Menü enthalten, das dem Benutzer mehrere Möglichkeiten für die Reaktion auf die Warnung einschließlich einer Sperrung der jeweils ausgeführten Funktion gibt. Die Sperrung kann dabei einmalig für die gerade ausgeführte Funktion oder auch für die Dauer des gerade laufenden Programms erfolgen. Andererseits kann der Benutzer trotz der Warnung die jeweils ausgeführte Funktion einmalig oder auf Dauer zulassen.

Die für die Ausführung der Prüfung gemäß Verfahrensschritt c) zugelassenen Dienstprogramme stehen zweckmäßig in einer Liste zugelassener Programme wie folgt:

CHKDSK, DEBUG, DISKCOPY, FDISK, FORMAT, MIRROR, RECOVER, REPLACE, SYS, UNDELETE, UNFORMAT.

Zusätzlich hat der Benutzer die Möglichkeit, weitere Programme, die er für zuverlässig hält, in die Liste einzugeben, und zwar solche Programme, die ebenfalls einen sektororientierten Zugriff auf Systembereiche benötigen, beispielsweise das bekannte Programm "PC TOOLS".

Patentansprüche

1. Verfahren zum Schutz von MS-DOS-Rechnern gegen Sabotageprogramme oder "Viren", gekennzeichnet durch die Verfahrensschritte:

a) bei Aufruf von sektororientierten Funktionen wird geprüft, ob der Aufruf vom Kern des Betriebssystems ausgeht,
b) bei positivem Ergebnis der Prüfung gemäß Schritt a) wird der Aufruf zugelassen,
c) bei negativem Ergebnis der Prüfung gemäß Schritt a) wird geprüft, ob der Aufruf von einem zugelassenen Dienstprogramm kommt,
d) bei positivem Ergebnis der Prüfung gemäß Schritt c) wird der Aufruf zugelassen,
e) bei negativem Ergebnis der Prüfung gemäß Schritt c) wird die Ausführung gesperrt und dem Rechnerbenutzer eine Warnung ausgegeben.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß zur Durchführung der Prüfung gemäß c) der Name des aufrufenden Programms festgestellt und mit einer Liste zugelassener Programme verglichen wird.

3. Verfahren nach Anspruch 2, dadurch gekennzeichnet, daß bei Aufrufen der EXEC-Funktion der Name des auszuführenden Programms abgespeichert und mit dem Namen des aufrufenden Programms verglichen wird.

4. Verfahren nach Anspruch 2 oder 3, dadurch gekennzeichnet, daß bei Aufruf einer der Funktionen "ABSOLUT DISK WRITE" oder "GENERIC BLOCK DEVICE REQUEST" oder "ROM-BIOS FIXED-DISK" der zugehörige INTERRUPT während der Initialisierungsphase umgeleitet, der Name des aufrufenden Programms geprüft und dann zum ursprünglichen INTERRUPT zurückgekehrt wird.

5. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß bei Aufruf des Plattentreibers oder der Funktion "EXECUTE DEVICE DRIVER REQUEST" festgestellt wird, ob ein Schreibzugriff auf den Systembereich vorliegt, und daß dann zur Prüfung, ob der Zugriff vom Kern kommt, festgestellt wird, ob zur Zeit eine MS-DOS-Funktion ausgeführt wird und ob sich die Transferadresse auf einen Kern-Datenpuffer bezieht.

6. Verfahren nach Anspruch 5, dadurch gekennzeichnet, daß zur Durchführung der Prüfungen der Plattentreiberaufruf dadurch umgeleitet wird, daß bei der Initialisierung ein neuer Plattentreiber angelegt wird, der die Prüfungen ausführt und bei positivem Ausgang den bisherigen Plattentreiber zur Ausführung des Zugriffs aufruft.

7. Verfahren nach einem der Ansprüche 1 bis 6, dadurch gekennzeichnet, daß die Warnung die Ausgabe eines optisch auffallenden Warnfensters auf dem Bildschirm des Rechners umfaßt und daß das Warnfenster die Ursache der Warnung angibt.

8. Verfahren nach Anspruch 7, dadurch gekennzeichnet, daß das Warnfenster ein Menü enthält, das dem Benutzer mehrere Möglichkeiten für die Reaktion auf die Warnung einschließlich einer Sperrung der jeweils aufgeführten Funktion angibt und eine Fehlerdiagnose liefert.

9. Verfahren nach einem der Ansprüche 1 bis 8, dadurch gekennzeichnet, daß für die Ausführung des Verfahrensschrittes c) die zugelassenen Dienstprogramme in eine Liste aufgenommen werden, die der Benutzer durch zusätzliche Programme ergänzen kann.

– Leerseite –